

วิธีตรวจสอบ E-mail ที่เป็นอันตรายเบื้องต้น

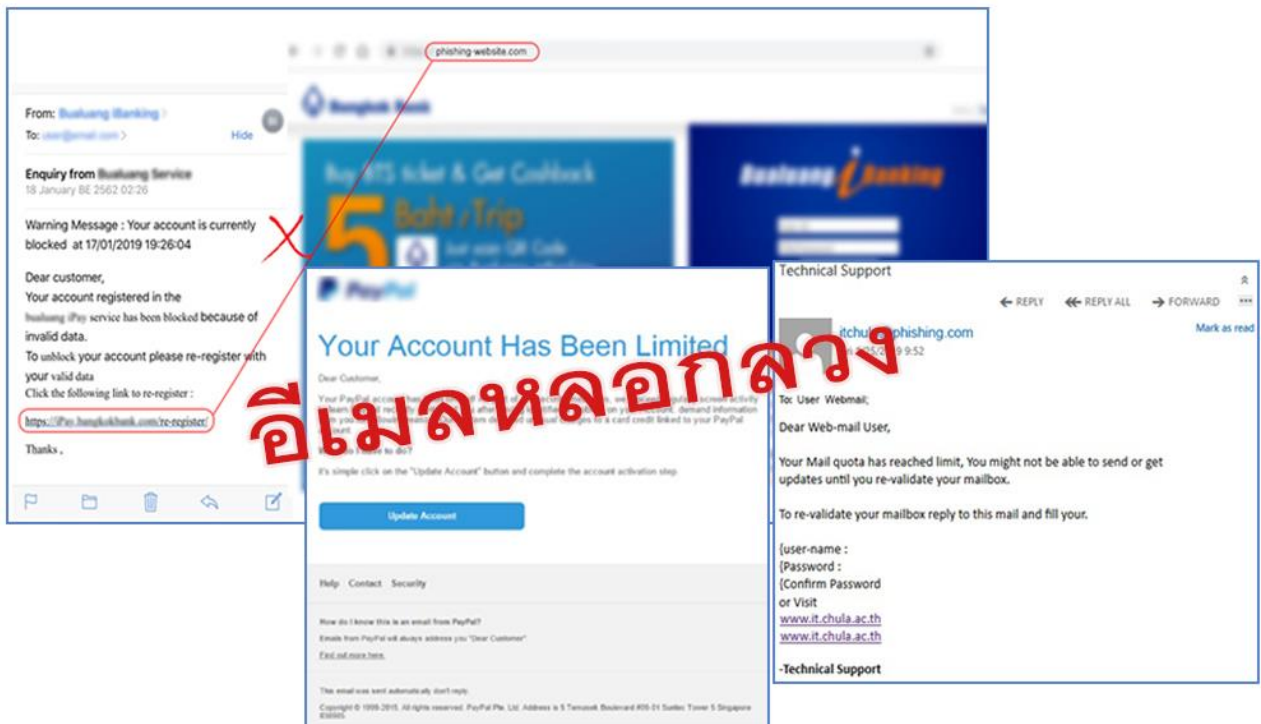
ในปัจจุบันอีเมลหลอกลวง (Phishing Email) ถือเป็นอีกหนึ่งวิธีที่ผู้ไม่หวังดีนำมาใช้เป็นช่องทางในการหลอกลวงผู้ใช้งานอีเมลให้หลงเชื่อเปิดอ่านหรือตอบกลับอีเมลฉบับนั้นเพื่อโจรกรรมข้อมูลของผู้ใช้งาน รวมทั้งอีเมลบางฉบับยังมีลิงก์เชื่อมโยงพาไปยังเว็บไซต์ที่เป็นอันตรายหรือหลอกลวง และอาจมีเอกสารหรือไฟล์แนบมาให้อีกด้วย หากผู้ใช้งานอีเมลไม่ระมัดระวังและหลงเชื่อเปิดอีเมลฉบับดังกล่าว อาจเป็นการติดตั้งโปรแกรมที่ไม่พึงประสงค์โดยไม่รู้ตัว และจากงานวิจัยของทาง Trend Micro พบว่า “ภัยคุกคามทางไซเบอร์มากกว่า 90% นั้น เริ่มต้นและถูกแพร่กระจายผ่านทางอีเมล” ดังนั้นเมื่อเราได้รับอีเมลหนึ่งฉบับจะแน่ใจได้อย่างไรว่าอีเมลดังกล่าวไม่ใช่อีเมลที่เป็นอันตรายหรืออีเมลหลอกลวงจากผู้ไม่หวังดี วิธีการตรวจสอบและการป้องกัน ทำได้อย่างไรบ้าง? ซึ่งในบทความนี้จะแนะนำวิธีตรวจสอบ E-mail ที่เป็นอันตรายเบื้องต้น ดังนี้

1. เมื่อได้รับอีเมลจากผู้ส่งที่เราไม่รู้จักให้ตรวจสอบข้อมูลผู้ส่งให้แน่ใจเสียก่อนว่าถูกต้องหรือไม่

หลายครั้งเมื่อเราได้รับอีเมลจากบุคคลที่ไม่รู้จักหรือได้รับข้อมูลที่ไม่ได้ร้องขอ อีเมลฉบับดังกล่าวอาจถูกส่งมาจากผู้ไม่หวังดี (Hacker) ซึ่งอาจมีไฟล์แนบหรือลิงก์เชื่อมโยงที่เป็นอันตรายมาด้วย ดังนั้นจึงขอแนะนำอย่าเปิดอีเมลฉบับดังกล่าว และถึงแม้จะเป็นผู้ส่งที่เรารู้จักหรือเคยติดต่อหากไม่เป็นการเสียเวลาก็ควรตรวจสอบที่อยู่อีเมลของผู้ส่งทุกครั้งว่าถูกต้องหรือไม่ เพราะอีเมลหลอกลวงส่วนใหญ่มักจะใช้คำสะกดที่ใกล้เคียงหรือคล้ายกับชื่อที่อยู่อีเมลของผู้ส่งตัวจริง

2. ไม่ตอบกลับหรือให้ข้อมูลสำคัญผ่านทางอีเมล

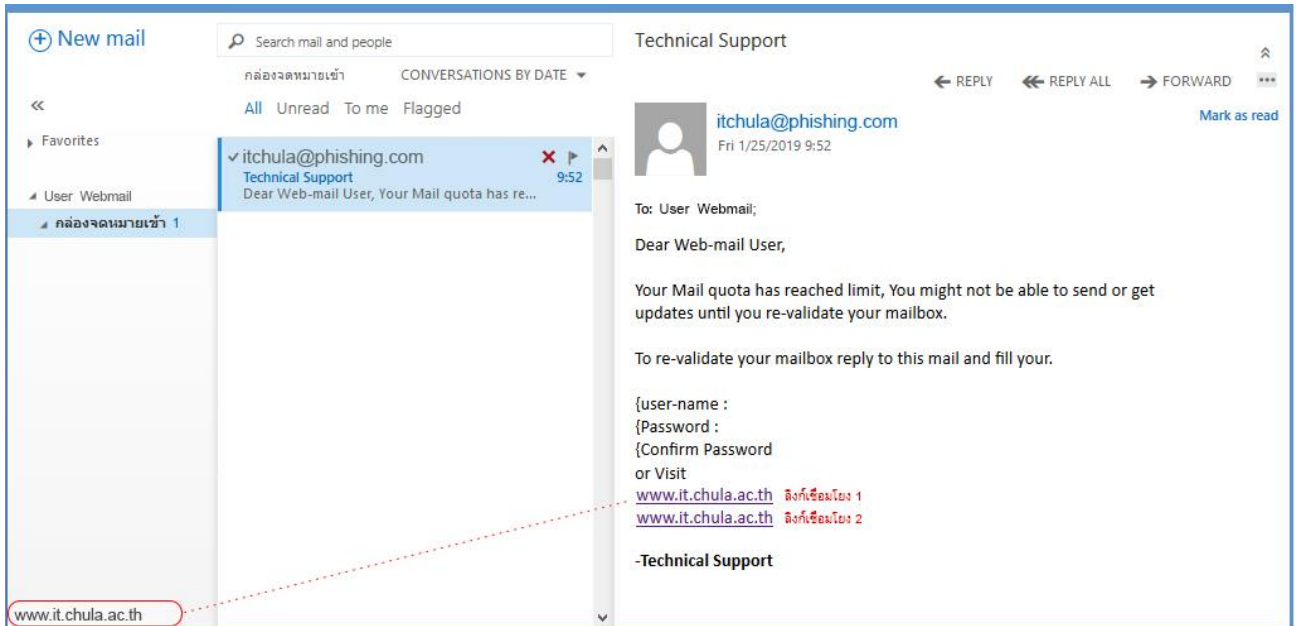
ลักษณะการหลอกลวงทางอีเมลที่พบได้บ่อยๆ คือการให้กรอกข้อมูลส่วนตัวหรือรายละเอียดบัญชีของผู้ใช้งาน อาทิเช่น รายละเอียดบัญชีธนาคาร, ชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) เป็นต้น โดยในความเป็นจริงแล้วผู้ให้บริการส่วนใหญ่จะไม่ยินยอมในการขอข้อมูลเหล่านี้ของผู้ใช้งาน ดังนั้นห้ามตอบกลับอีเมลที่มีเนื้อหาลักษณะดังกล่าวเด็ดขาด หากไม่แน่ใจให้ทำการสอบถามจากผู้ให้บริการโดยตรง



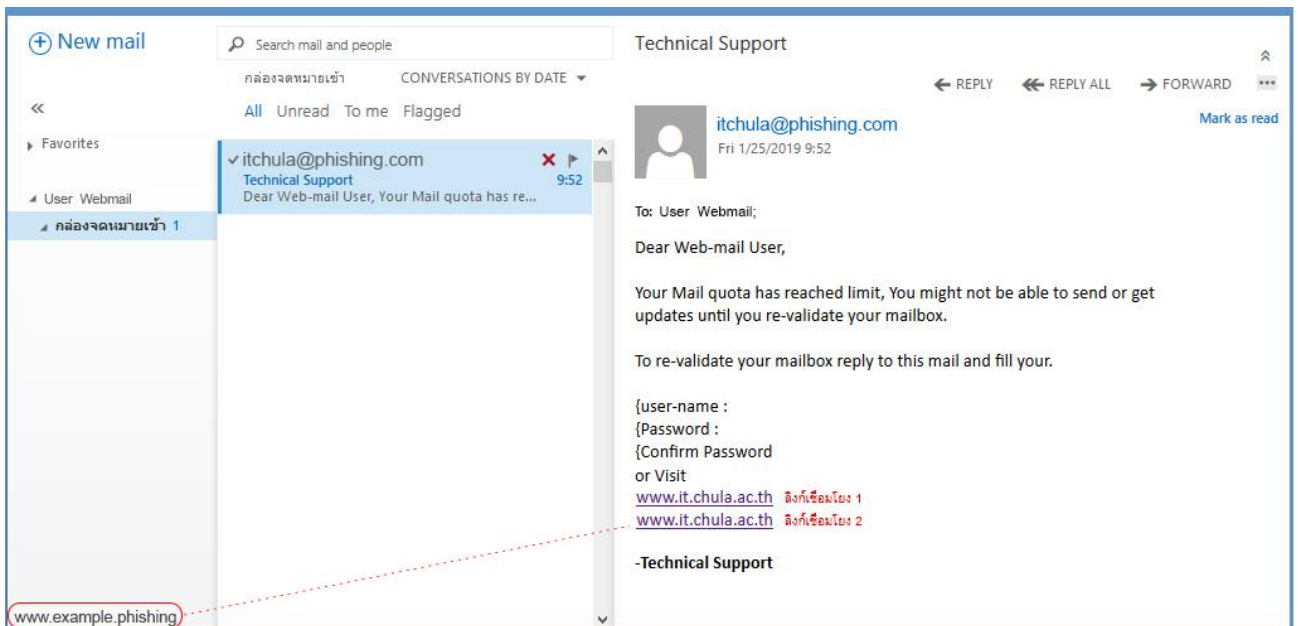
รูปที่ 1 ตัวอย่าง อีเมลหลอกลวง

3. ตรวจสอบลิงก์เชื่อมโยงที่แนบมาในอีเมลทุกครั้งก่อนคลิก

หากมีลิงก์ที่แนบมาในอีเมล ให้สังเกต URL ทุกครั้งก่อนคลิก และเมื่อลิงก์ถูกเชื่อมโยงไปยังเว็บไซต์ ให้ตรวจสอบ URL ด้านบนของเว็บเบราว์เซอร์อีกครั้ง เพื่อให้แน่ใจว่า URL ถูกต้องไม่ใช่เว็บไซต์ปลอม



รูปที่ 2 URL ของลิงก์เชื่อมโยง 1

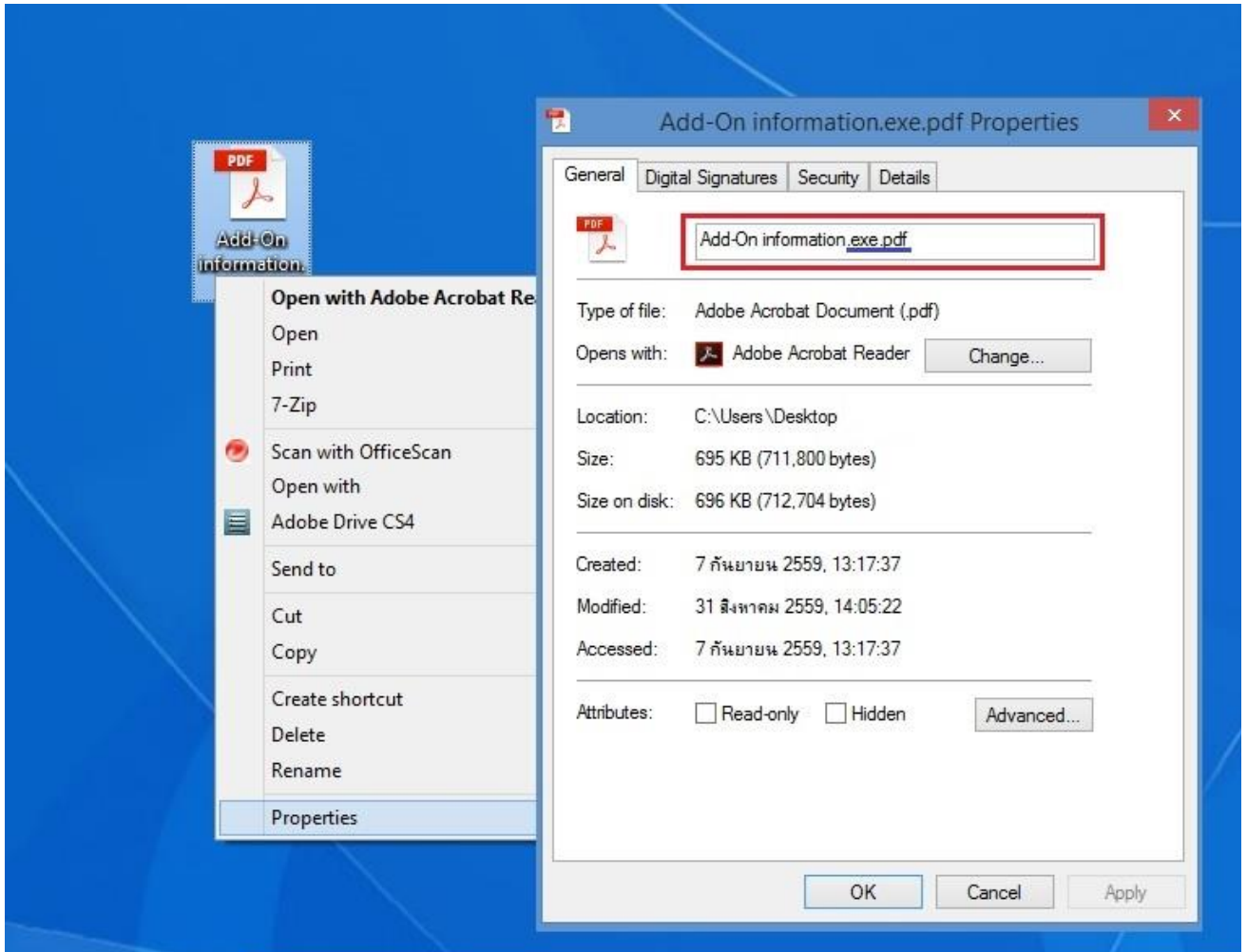


รูปที่ 3 URL ของลิงก์เชื่อมโยง 2

จากรูปที่ 2 และ 3 จะเห็นได้ว่าถ้าไม่ได้สังเกต URL ด้านซ้ายล่าง ผู้ใช้งานอีเมลอาจคลิกไปยังเว็บไซต์ที่ผิดได้โดยไม่รู้ตัว เพราะฉะนั้นอย่าลืมตรวจสอบทุกครั้งก่อนทำการคลิก โดยวิธีการตรวจสอบเพียงแค่เลื่อนเมาท์ไปไว้ด้านบนของลิงก์ดังกล่าวแล้วสังเกตตามในรูปภาพได้เลย

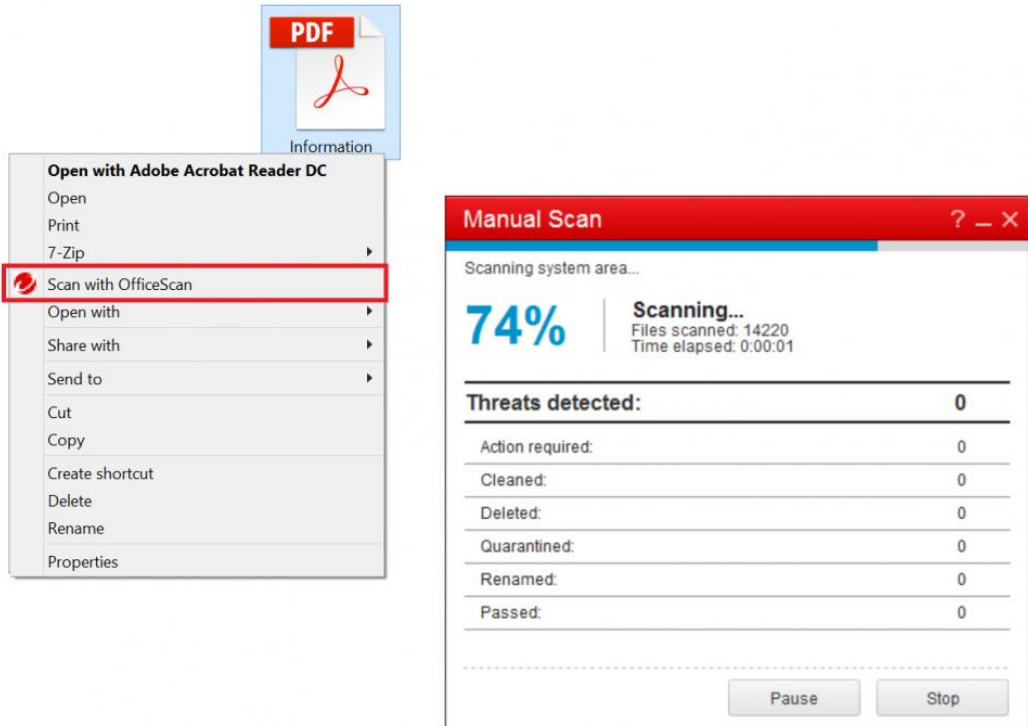
4. ตรวจสอบเอกสารหรือไฟล์แนบทุกครั้งก่อนเปิดอ่าน

เมื่อใดก็ตามที่คุณได้รับอีเมลที่มีเอกสารหรือไฟล์แนบมาด้วย หากต้องการดาวน์โหลดไฟล์ดังกล่าว ต้องมั่นใจว่าเครื่องคอมพิวเตอร์ของคุณมีการติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนเครื่องคอมพิวเตอร์ เพราะไฟล์ที่แนบมานั้นอาจประกอบไปด้วยโปรแกรมที่ไม่พึงประสงค์ (Malware) หรือโปรแกรมที่ใช้ทำการเข้ารหัสหรือล็อกไฟล์บนเครื่องคอมพิวเตอร์ (Ransomware) ซึ่งอาจเป็นอันตรายกับเครื่องคอมพิวเตอร์ของคุณได้ ดังนั้นเมื่อดาวน์โหลดไฟล์ดังกล่าวเสร็จแล้วให้ทำการสแกนไฟล์ (Manual Scan) ด้วยโปรแกรมป้องกันมัลแวร์ และตรวจสอบนามสกุลของไฟล์นั้นทุกครั้งก่อนเปิดอ่าน



รูปที่ 4 การตรวจสอบนามสกุลของไฟล์แนบ

จากรูปที่ 4 จะเห็นได้ว่าไฟล์ที่ถูกส่งมาจากอีเมลอาจถูกแนบมาในรูปแบบของ .pdf แต่ถ้าผู้ใช้งานอีเมลตรวจสอบนามสกุลของไฟล์ดังกล่าวเต็มที่ ก็จะทราบว่าที่จริงแล้วมีนามสกุล .exe ที่เป็นนามสกุลของไฟล์ติดตั้งโปรแกรมซ่อนอยู่ ซึ่งบางทีโปรแกรมดังกล่าวอาจเป็นโปรแกรมที่ไม่พึงประสงค์หรือโปรแกรมที่ใช้ทำการเข้ารหัสหรือล็อกไฟล์บนเครื่องคอมพิวเตอร์ (Ransomware) เลยก็เป็นได้ โดยวิธีการตรวจสอบนามสกุลไฟล์ทำได้โดยการคลิกขวาที่ไฟล์ดังกล่าวแล้วเลือก 'Properties' หลังจากนั้นก็มีหน้าต่าง Properties ปรากฏขึ้นมา



รูปที่ 5 การการสแกนไฟล์ (Manual Scan)

และหากเครื่องคอมพิวเตอร์มีการติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) ของทางมหาวิทยาลัยอยู่แล้ว สามารถทำการสแกนไฟล์ (Manual Scan) โดยการคลิกขวาที่ไฟล์ดังกล่าวแล้วเลือก 'Scan with OfficeScan' ได้เลย

ขอขอบคุณข้อมูลดีๆ จาก : สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย